



# **What's New in NISP Information Assurance-- 2005**

**Defense Security Service  
NCMS National  
June 2005**

# Topics

- **ISP Leadership, Email Addresses & Website**
- **FAST Tool**
- **NISP Chapter 8 Tool**
- **Office of the DAA**
- **SIPRNet**
- **Final Accreditation Letters**
- **On-Line Chapter 8 for Industry Course**
- **ISL 05L-1**
- **Clarifications**

# **Leadership in Industrial Security**

- **Deputy Director for Industrial Security—Mary Griggs**
- **Assistant Deputy Directors for:**
  - **Policy—Steve Lewis**
  - **Field Services—Valerie Heil**
  - **Field Operations—Rick Lawhorn**
  - **Critical Infrastructure Protection—Mike Berry**
  - **Office of Designated Approving Authority**
  - **Research Technology and Protection**

# **Leadership in Industrial Security**

- **Assistant Deputy Director for Field Operations (Rick Lawhorn)**
- **Regional Directors for:**
  - **Northern Region (Al Buccigrosso)**
  - **Capitol Region (Steve Hampton)**
  - **Southern Region (Tim Sartin)**
  - **Western Region (John Whitecotton)**

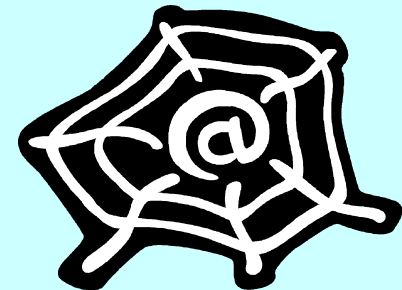
# DSS Email Addresses

- **Dropped the: @mail**
- **Changed to :**  
**kenneth.quigley@dss.mil**
- **Address is not case sensitive.**



# Information Assurance Website

- **[www.dss.mil/infoas/index.htm](http://www.dss.mil/infoas/index.htm)**
- **Posting useful documents**
  - NSA Documents
  - Encryption Doctrines
  - Security Configuration and Analysis Template
  - Briefings
  - Other helpful documents
- **Because FOUO, must have password for some documents**



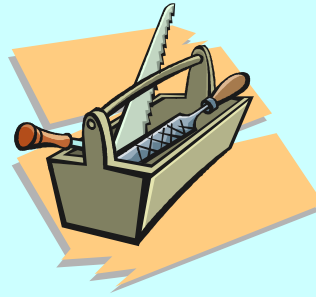
# Information Assurance Website

- For password, if not FSO, must obtain FSO approval
- FSO email following information to [account.request@dss.mil](mailto:account.request@dss.mil)

- Facility Name
- Facility Address
- Cage Code
- FSO Name
- FSO E-mail Address
- FSO Telephone Number
- Employee's Name
- Employee's Phone Number
- Employee's E-mail Address

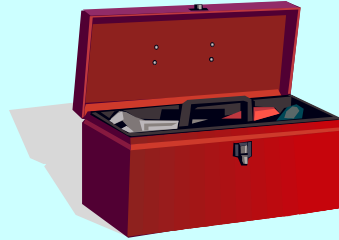


# FAST Tool



- **Electronic SSP generation tool**
- **Question and answer format**
- **Beta Testing in progress**
- **177 Contractor sites across nation**
- **Will enable industry to build detailed SSPs and assist in leading to more timely accreditations**

# NISP Chapter 8 Tool



- **Capitol Region beta testing is completed**
- **System configuration verification tool**
- **Will provide verification for Windows NT, XP, 2000 or 2000 Active Directory**
- **Provides a method for industry to conduct a self-assessment for compliance**
- **Reports generated in html format, but can be viewed with any text-editing tool**
- **DSS will utilize during C&A and inspections**

# **ODAA**

## **(Office of Designated Approving Authority)**

- **Currently in development**
- **Assistant Deputy Director, ODAA.**
- **Under the auspices of the ISP**
- **Designed to consolidate the DAA activities**
- **Centrally monitor and manage policies, procedures, workflow, timeliness, quality**
- **Tech Directors report to ODAA**



# **ODAA**

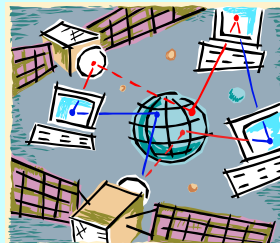
## **(Office of Designated Approving Authority)**

- **Centralized accreditation of System Security Plans (SSPs)**
- **Improving consistency and timeliness of C&A process**
- **Oversee development of automated tools**
- **Research issues & new technology**



# SIPRNet

- **Reminder for those approved for SIPRNet**
- **SIPRNet Connection Questionnaire (SCQ) dtd 4/13/04**
  - **Contractor completes--Questions 1, 2, 3 & 6 for contractors are “Yes”—provide details**
  - **Signed by DSS DAA**
- **Consent to Monitor letter: contractor completes**
- **Final Accreditation letter and SCQ mailed or electronically returned to contractor**
- **Contractor mails complete SIPRNet Package to DISA**



# **Final Accreditation Letters**

- **Where possible, DAAs are emailing final accreditation letters**
- **If sent directly to the facility the ISR and FOC will be copied**
- **If ISSM or FSO email address are unknown, will be sent electronically to the ISR for forwarding to the facility**
- **Remember to include your email address**



# **On-Line Chapter 8 for Industry Course**

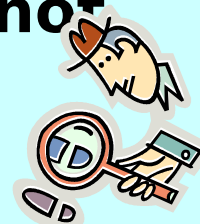


- **Now on a computer near you “anytime-anywhere”**
- **In a 90-Day trial period**
- **Content same as instructor led course, to replace instructor led course**
- **Upon successful completion of final exam, students will be issued a Certificate of Completion**
- **Completion satisfies training requirements of ISL 01L-1, Question 8**
- **To sign up go through ENROL on the DSSA website**
- **NOTE: Must complete prerequisite course, Information System Security Basics, currently available on ENROL**

# ISL 05L-1

## Item #12

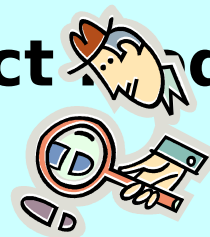
- **Auditing Clarification:**
  - **Systems capable of auditing must have it enabled**
  - **Must make every effort to meet Chap 8 auditing requirements:**
    - **Upgrading operating system (O/S) as appropriate**
    - **Obtaining third party software, if necessary**
  - **Exception applies only when GCA requires use of an O/S not capable of meeting Chap 8 audit requirements**
  - **In such instances, NISPOM waiver is not required**



# **ISL 05L-1**

## **Item #12 (cont.)**

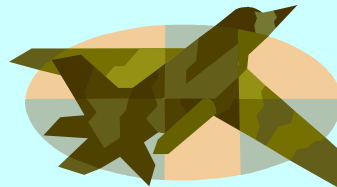
- Provide contract documentation from the GCA: DD Form 254, classification guidance and/or a memorandum that directs use of O/S**
- Format: “contractor is required to use Windows 98”, followed by rationale**
- Signed by the Contracting Officer, COR or COTR**
- Formal contract modification is not necessary**



# **ISL 05L-1**

## **Item #13**

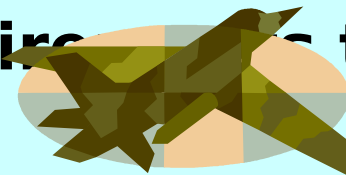
- **Tactical/Embedded/Special Purpose Systems:**
  - **Examples:**
    - **Local Management Devices - Key Processors (LMD-KPs)**
    - **Guidance sets for command and control systems**
    - **Weapon platforms such as missile systems, tanks and submarines.**
  - **Includes prototypes remaining under custody of the contractor**



# ISL 05L-1

## Item #13 (cont.)

- **GCA is responsible for developing security requirements**
- **If not provided, the ISR will direct contractor to request them from the GCA**
- **Security requirements should specify:**
  - **Components considered part of the system**
  - **Security requirements to be implemented**



# ISL 05L-1

Item #13 (cont.)

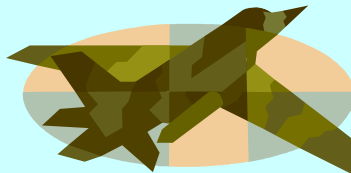
- **If not furnished, the contractor will submit procedures to DSS to protect the system and classified information against unauthorized disclosure or loss**
- **If ISR notes vulnerability that could lead to potential compromise, will note to GCA**



# **ISL 05L-1**

**Item #13 (cont.)**

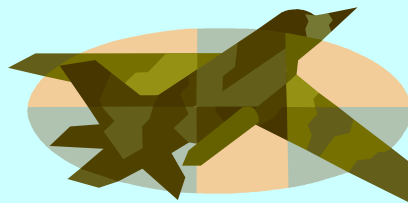
- **Systems will not require DSS accreditation**
- **Contractor will not be held to NISPOM Chapter 8 standards**



# **ISL 05L-1**

## **Item #13 (cont.)**

- **Test equipment utilized at contractor facilities to test various deliverable components will be accredited only if it has storage media or user-addressable non-volatile memory and processes classified.**



# **ISL 05L-1: IS Questions**

## **Item #15**

- **Definition of single-user standalone:**



- **Physically and electronically isolated from all other systems**
- **Use by one person only; assigned to one individual**
- **Single-user if individually assigned removable hard drives & system sanitized between users**
- **IT support personnel not considered users**

# **ISL 05L-1: IS Questions**

## **Item #15 (cont.)**

- **At PL-1 NISPOM Para 8-103g satisfied by submitting written statement:**



- **SSP has been implemented**
- **Specified security controls are in place and properly tested**
- **IS is functioning as described in the SSP**
- **Test plan not required, but helpful with consistency if self-certifying**

# ISL 05L-1: IS Questions

## Item #15 (cont.)

- **With DSS Approval, ISSM may serve for multiple facilities within a defined area**

- **Approx. one-hour ground travel time**
- **Number and complexity appropriate to the ISSM's oversight capability**
- **On a temporary basis and with DSS approval, ISSM may self-certify systems for facilities greater than one-hour**
- **Provide plan detailing how ISSM responsibilities will be managed**



# ISL 05L-1: IS Questions

## Item #15 (cont.)



- **IS being upgraded can be booted from a floppy or CD-ROM if:**
  - **Protected to the level of the information system**
  - **Used in a read-only configuration**
  - **Best boot from internal drive as security controls can be circumvented by external media**
- **MOU not required**
  - **When accredited mobile systems are relocated to government activities or test sites**
  - **Contractor must have a signed “Letter Acknowledging Relocation of IS by Government Activity” prior to shipment**

# ISL 05L-1: IS Questions



- **Use of new media when doing trusted downloading**
- **Review and testing of unclassified software**
- **Control of foreign government information**
- **See ISL 05L-1**

# Clarifications

- **Under discussion with DISA:**
  - **Contractors with DISN connections will be required to follow DISA STIGs\***
- **As a rule, Memorandum of Understanding (MOU) and Network Security Plan (NSP) separate documents**
- **Audit TacLANes only if GCA requests**
- **Virus definition updates should be recorded in the significant action/maintenance log**



# Summary

- Updated what's new
- Watch for additions to website